COMMON CRITERIA PROJECT
IMPLEMENTATION STATUS
PANEL

Panelists:
The panelists are representatives from the Common Criteria (CC) sponsoring organizations who are active participants in one or more of the current CC trial-use and implementation projects.

Lynne Ambuel
National Security Agency, US
ambuel@dockmaster.ncsc.mil

Klaus Keus
BSI/GISA, Germany
keus@bsi.de

Murray Donaldson
Communications-Electronics
Security Group, United Kingdom
mgdonal@itsec.gov.uk.

Frank Mulder
Netherlands National Communications
Security Agency
mulder@nlncsa.minbuza.nl

Robert Harland
Communications Security
Establishment, Canada
rharland@cse.dnd.ca

Jonathan Smith
Gamma Secure Systems, United Kingdom
jsmith@gammassl.co.uk

Abstract

Common Criteria (CC) trial version 1.0 was completed in January 1996 and has entered into an active trial-use and implementation phase during 1996. Along with numerous trial evaluations of both IT security products and Protection Profiles against the CC by the sponsoring organizations in both North America and Europs, a number of related implementation projects have been initiated. These projects include:

- preparation of a common evaluation methodology,
- development of a framework for mutual recognition of the results of evaluation by the participating organizations, and
- study and development of prospective alternative approaches to evaluation.

In addition, extensive comments are being received from the IT security community review process. Expected output of all of this activity is a set of recommendations for revision of the CC to the definitive version 2 during 1997 and its acceptance as an ISO international standard.

The members of this panel represent the Common Criteria Implementation Board, the Common Evaluation Methodology Editorial Board, the Mutual Recognition Working Group, and the Assurance Approaches Working Group. The panelists will jointly discuss the CC trial version's structure and contents, the status and results to date of the trial-use and implementation activities, the planned future of the project, and the expected impact of all of this work on the US and international IT security communities.

Background

The Common Criteria Project is nearing the culmination of seven years of work in several nations to achieve a set of standard criteria for specifying IT security products and for performing evaluations on them. The goal is to provide a "level playing field" for both national and multi-national IT developers that will result in broader availability of IT products with known and trusted security characteristics for general use in both government and private organizations.

The original "Trusted Computer System Evaluation Criteria" (TCSEC) or "Orange Book", waas adopted by the US Department of Defense in 1985. This document has been used by the National Security Agency (NSA) for security product evaluation until the present. The known limitations of the TCSEC motivated NSA and the National Institute of Standards and Technology to embark on the Federal Criteria Project in early 1991 to create a more flexible set of criteria that can take into account advances in security technology and widespread inter-connectivity of computers. Federal Criteria draft version 1 was published in late 1992. Several European nations individually, then jointly, were working on their own criteria and evaluation programs during the same period, resulting in the initial publication of the Information Technology Security Evaluation Criteria (ITSEC) in mid-1990, with the current version delivered a year later. The Canadians also had begun their own criteria development activity in the late 1980's, and the last version of the Canadian Trusted Computer Product Evaluation Criteria (CTCPEC) was published in early 1993.

The US, Canada and the Europeans in 1993 agreed that it was time to work together to resolve any differences in approach and develop a single Common Criteria that could be contributed to ISO for use world-wide as an international standard. The Common Criteria Project thus began in the Fall of 1993.

Current Status

The CC was first published in rough draft for limited community review in mid 1994. It was extensively revised and again circulated, this time very widely, in late 1994. Based on input from the ISO committee also working on an international criteria, public review and comments, and the results of an international workshop, CC version 1.0 was published in January 1996. Part 1 of the CC had already been accepted by ISO as a working draft of its own criteria Part 1. Upon publication of CC version 1.0, ISO accepted all three principal parts of the CC as its second level "committee draft". This marked a major break-through, as for the first time there is a single internationally-accepted set of IT security criteria.

The CC Project Sponsoring Organizations created the CC Implementation Board (CCIB) to coordinate a variety of implementation activities, including trial evaluations, and prepare for the definitive version. The CCIB will collect and dispose of all identified problems and proposed changes to the CC during the trial-use period, whether from community review or from use of the CC for trial evaluations and preparation of evaluation methodology. The CCIB is also responsible for publicizing the CC and seeking its wide acceptance in the community of users, developers and academics. By the end of 1996, the CCIB will have collected all input on needed changes and will prepare a set of recommendations for preparation of the definitive version 2.0.

There are a large number of trial developments and evaluations underway based on CC version 1.0. In most of the participating nations, one or more trial evaluations of products are being conducted against the CC in parallel to their evaluations against the existing base criteria. In addition, CC-based Protection Profile requirement sets are being created for new products, such as firewalls and smartcards, as well as replacements for existing requirement sets in the TCSEC, ITSEC and CTCPEC.

The Common Evaluation Methodology Editorial Board (CEMEB) was also created in early 1996 to develop an agreed methodology that would represent the accepted way to perform product evaluations in the participating nations. There are three "legs" that support mutual recognition of each nation's security product evaluations:

- The CC itself, consisting of common requirements for security functions and assurance,
- A common approach or method for performing the evaluations, and
- Known competent evaluators to do the work in each participating nation.

Each nation or region performing product evaluations now has their own methodology. These methods have similar approaches and activities that constitute their evaluations, which must now be analyzed and the commonly-needed elements described. The CEMEB will develop and test these detailed evaluation methods.

A Mutual Recognition Working Group was formed.in mid-1996 to explore the legal, procedural and technical basis for each participating nation to recognize the IT security evaluation work of the other participants. This is a complex and potentially difficult topic because of differing legal structures, governmental policies, and current approaches. Currently, only a few bilateral agreements exist. It is expected that this group will continue to work over the next few years to put the broader agreements in place and resolve practical difficulties.

One CC-related group has been formed to move beyond the current evaluation-based assurance paradigm for commercially-oriented IT products. The major objective of the Assurance Approach Working Group (AAWG) is to investigate alternative approaches for gaining assurance that IT products and systems meet their security requirements. The group seeks to find, in the existing methods of product development or methods of validating them, alternate requirements to satisfy the assurances objectives expressed in the CC. This group is working to develop and test faster and more timely ways to provide trusted commercial products.

Plans

The ultimate plan for the CC is to gain information from application and study of the current version 1.0 to prepare a definitive version that can be turned over to ISO for use and maintenance as an international standard. Preparation of version 2.0 is expected to begin in early 1997. Continuing development of the common evaluation methodology and procedures for mutual recognition will proceed over the next few years, and the CC will be introduced into evaluation schemes in North America, Europe and perhaps elsewhere in the world.